Exhibit 1

BRIEFING ROOM

Background Press Call by Senior Administration Officials on Russia

APRIL 15, 2021 • PRESS BRIEFINGS

Via Teleconference

9:36 A.M. EDT

SENIOR ADMINISTRATION OFFICIAL: Hi everyone. Thanks for joining us this morning. We're going to be on background today, with comments attributed to "senior administration officials," and the contents of this call are going to be embargoed until its conclusion.

We have three speakers today for you. [Redacted.] [Senior administration official], we'll turn it over to you for opening comments, and then we'll hear from [senior administration officials], and then we're happy to take your questions.

SENIOR ADMINISTRATION OFFICIAL: Thanks everybody for joining us this. I'll spend a few minutes at the top laying out the context for today's actions and then some of the specific measures we've undertaken.

We've been clear that we seek a relationship with Russia that that is stable and predictable. We do not seek, we do not desire a downward spiral. We think we can and should avoid that. But we have also been clear, publicly and privately, that we will defend our national interests and that we will impose costs on Russian government actions that seek to harm our sovereignty.

In his first conversation with President Putin not long after his inauguration, President Biden raised our strong concerns about a number of harmful foreign activities by Russia and indicated that the United States would respond. On March 2nd, the Biden administration, in coordination with several key allies and partners, announced our response to Russia's use of a chemical weapon to poison Aleksey Navalny. Then, earlier this week, the President spoke with President Putin again and told him, true to his word, that the United States would in fact be executing responses to the cyber intrusion of SolarWinds and the interference in the 2020

election.

This week and today, that is what we are doing; we are taking additional actions to respond to what the Russian government and its intelligence services have done to directly target American sovereignty.

There will be elements of our responses to these actions that will remain unseen. Our actions announced today constitute our public response, which we intend to be understood as resolute but proportionate.

On SolarWinds, we're formerly naming the Russian Foreign Intelligence Service — the SVR — as the perpetrator of the broad-scope cyber espionage campaign that exploited the SolarWinds Orion platform and other information technology infrastructures.

The SVR unit, APT29, Cozy Bear, the Dukes — known by all of those names — we are attributing as the actor that conducted this intrusion. The U.S. intelligence community has high confidence in its assessment of attribution to the SVR. This is an update to the January 5th, 2021, assessment by the previous administration that this incident was, quote, "likely of Russian origin."

Sanctions are one component of today's response. Today, President Biden signed a new sanctions executive order that provides strengthened authorities for the administration to respond to and deter Russia's harmful foreign activities. It sends a clear signal to the Russian government that we will not accept its destabilizing behavior that harms the United States, our people, our allies and partners, and that we will respond with economically impactful costs if these activities continue or escalate.

Under the new EO, Treasury today has issued a directive that prohibits U.S. financial institutions from participation in the primary market for ruble or non-ruble denominated bonds issued after June 14th, 2021, by the Central Bank of the Russian Federation, the National Wealth Fund of Russia, or the Ministry of Finance. This directive provides authority for the U.S. government to expand sovereign debt sanctions on Russia as appropriate.

Also under the new EO, Treasury has today designated six Russian companies that provide support to the SVR cyber program and other Russian intelligence agencies' cyber programs, ranging from providing expertise, to developing tools and infrastructure, to facilitating malicious cyber activities.

Importantly, there are elements of this new EO that give us additional authorities that we are

not exercising today. We would prefer not to have to deploy these authorities, but the scope of the EO and it potential to cause meaningful impact should send a clear signal that continued harmful foreign activities — including further election interference, further malicious cyber activities — are unacceptable, and we are prepared, going forward, to impose substantial and lasting costs if this behavior continues or escalates.

Under other sanctions authorities today, Treasury also sanctioned 32 entities and individuals carrying out Russian government-directed attempts to influence the 2020 U.S. presidential election and to pursue other forms of disinformation and influence campaigns against partners, allies, and other governments.

This action seeks to disrupt the coordinated efforts of Russian officials, proxies, and intelligence agencies to delegitimize democratic electoral processes.

Furthermore, Treasury — in partnership with the EU, UK, Australia, and Canada — today sanctioned eight individuals and entities associated with Russia's ongoing occupation and repression in Crimea. And the United States is expelling 10 Russian officials from Russia's Washington, D.C., diplomatic mission.

At the same time, we're taking a number of steps to help allies and partners identify cyberattack perpetrators and strengthen our cybersecurity partnerships with like-minded nations.

Finally, let me offer an update on reports of bounties on U.S. soldiers in Afghanistan. The United States intelligence community assesses, with low to moderate confidence, that Russian intelligence officers sought to encourage Taliban attacks against U.S. and coalition personnel in Afghanistan in 2019 and perhaps earlier, including through financial incentives and compensation. U.S. intelligence community agencies have low to moderate confidence in this judgment, in part because it relies on detainee reporting and due to the challenging operating environment in Afghanistan.

Our conclusion is based on information and evidence of connections between criminal agents in Afghanistan and elements of the Russian government. This information puts a burden on the Russian government to explain its actions and take steps to address this disturbing pattern of behavior.

The safety and wellbeing of U.S. military personnel and that of our allies and partners is a matter of the absolute highest U.S. national security interest. Our men and women in uniform have defended our country from harm and promoted our interests and values around the

world. They will continue to do so, and we cannot and will not accept the targeting of our personnel like this.

As we take these actions, we also want to be clear that we have no desire to be in an escalatory cycle with Russia. We intend these responses to be proportionate and tailored to the specific past activities, past actions that Russia has taken. We have indicated that we seek a stable and predictable relationship going forward.

President Biden spoke with President Putin earlier this week and conveyed that directly. And in that spirit, he proposed a summit meeting in the coming months, in a third country in Europe, to discuss the full range of issues in our relationship. The Russians have not responded to that to say whether they will — whether President Putin will participate in such a summit. But we believe that, in the coming months, it will be vital for the two leaders to sit down to discuss the full range of issues facing our relationship. And as responsible — and it is the responsibility of the leaders of significant countries, like Russia and the United States, to sit together to find a stable and effective way forward and to stop any kind of escalatory cycle from spinning out of control.

I will stop there and turn it over to my colleagues.

SENIOR ADMINISTRATION OFFICIAL: Thanks, [senior administration official]. So, as [senior administration official] just underscored, President Biden has been clear about his desire for a relationship with Russia that's stable and predictable. He's also been clear that we'll defend our national interests and impose costs for Russian government actions that seem to harm — that seek to harm our sovereignty.

And so that's the context in which we're taking action today to impose tailored and proportionate costs in the Russian sovereign debt market for actions directed by President Putin that have directly targeted American sovereignty.

This is a matter of principle. There's no credible reason why the American people should directly fund Russia's government when the Putin regime has repeatedly attempted to undermine our sovereignty.

To be clear, before we took this action, our sanctions prohibitions only prevented U.S. persons from purchases of non-ruble denominated debt at issuance. This meant the vast majority — over 80 percent — of the sovereign debt that Russia issues — the ruble-denominated portion — was untouched by our sanctions regime.

We've now expanded our prohibitions to cover this space, and we're also delivering a clear signal that the President has maximum flexibility to expand the sovereign debt prohibitions if Russia's maligned activities continue or escalate.

For now, though, we want to be clear that this prohibition only applies to newly issued ruble sovereign debt in the primary market, and not to the secondary market or existing sovereign debt holdings.

You should also know that the prohibition comes into effect on June 14 of this year. The intent — the intent here is to allow for an orderly process and to limit spillovers to U.S. or global financial markets.

In terms of how this action imposes costs: Remember, this is the main market that funds the Russian government. The ruble-denominated sovereign debt market is about 185 billion in size, about a quarter of these bonds are owned by foreign investors.

Judging from history, removing U.S. investors as buyers in this market can create a broader chilling effect that raises Russia's borrowing costs, along with capital flight and a weaker currency. And all of — all of these forces have a material impact on Russia's growth and inflation outcomes.

But to underscore: The speed and magnitude of that negative feedback loop is a function of Russia's choices. And just to repeat what [Senior Administration Official] said, we're not looking for escalation; we're providing a proportionate and tailored response. And we believe it's in our interest to find a stable and predictable way forward in the relationship.

Let me turn it now over to [senior administration official].

SENIOR ADMINISTRATION OFFICIAL: Thank you, [senior administration official]. Good morning all.

So building on [senior administration official]'s comments regarding the United States formally naming the Russian Foreign Intelligence Service, SVR, as responsible for the SolarWinds hack: The U.S. Intelligence Committee (inaudible) has high confidence in its assessment of the attribution to the SVR.

There are two aspects to the U.S. response to SolarWinds. First, naming and imposing costs on the perpetrator of SolarWinds. And second, strongly affirming the importance of an open, interoperable, secure, and reliable Internet.

So on the first aspect, building on the attribution and, as [senior administration official] noted, Treasury's designation of six Russian technology companies that provide support to the Russian Intelligence Service's cyber program, ranging from providing expertise to developing tools and infrastructure to facilitate those malicious cyber activities. They're being designated — the companies — for operating in the technology sector of the Russian Federation economy. And we will continue to hold those companies accountable for that behavior.

Second, the SVR's compromise of SolarWinds and other companies highlights the risks posed by Russia's efforts to target companies worldwide through supply chain exploitation. Those efforts should serve as a warning about the risks of using information and communications technology and services supplied by companies that operate or store user data in Russia, or rely on software development or remote technical support by personnel in Russia.

The U.S. government strongly encourages all U.S. companies using communications or technologies supplied by companies with ties to Russia to evaluate the security of their infrastructure and be aware of the potential for future U.S. action that may affect their operation.

The U.S. government is evaluating whether to take action under Executive Order 13873 to better protect our communications and technology supply chain from further exploitation by Russia.

The United States is not alone in facing malicious Russian cyber activity. And you may have noted both Australia and the European Union statement of support for the attribution and the need to counter that malicious activity this morning.

As I noted, the second and key part of this morning's activity are the U.S. strongly affirming the importance of an open, interoperable, secure, and reliable Internet. Russia's actions run counter to that goal, which is shared by many of our allies and partners.

So, to strengthen our collective approach to bolstering cyber security, we're announcing two important steps.

First, the United States is strengthening our efforts to promote a framework of responsible state behavior in cyberspace and to cooperate with allies and partners to counter malign cyber activities, such as what we've seen perpetrated by Moscow.

We're providing a first-of-its-kind course for policymakers worldwide on the policy and

technical aspects of publicly attributing cyber incidents that will be inaugurated this year at the George C. Marshall Center in Germany.

Second, we're reinforcing our commitment to collective security in cyberspace. The Department of Defense hosts an important annual cyber exercise to build security and cyber operators and overall capability. We will be inviting — and the UK, France, Denmark, and Estonia have agreed to join in the planning for this year CYBER FLAG exercise.

The exercise will build a community of defensive cyber operators and improve overall capability of the U.S. and our allies to identify, synchronize, and respond in unison against malicious cyberspace activities targeting our critical infrastructure and key resources. This effort is intended to reinforce again our commitment to the security of our allies and partners.

As the SolarWinds incident has shown, we have to build those domestic and international partnerships and threat intelligence sharing to ensure we can identify, defend against, and mitigate malicious cyber activity from Russia and other adversaries.

Our efforts this morning are designed to be proportionate and tailored to counter the activities we experienced in the malicious cyber activities in the SolarWinds hack, as well as to build collective security with our allies.

And, with that, I'll turn it over for your questions.

Q Hey. Thank you. Question — a couple questions. Why list the reported Taliban attacks if there's low to moderate confidence?

And second, on the — if I understood right, the Treasury financial impacts don't go into effect until June 14th. Why is there a delay on that?

And third, how did you pick the Russians that are being expelled? Thank you.

SENIOR ADMINISTRATION OFFICIAL: Thanks. I'll take the first and third questions, and I will hand it over to [senior administration official] for the second one.

With respect to the question of the reports of bounties or financial compensation on — you know, provided to Afghans to kill Americans or coalition troops, as I noted in my opening comments, the IC has low to moderate confidence in this, both because it's based in part on detainee reporting and because of the difficult operating environment in Afghanistan.

The actions that we have announced today are in response to the cyber intrusions and the election interference. We have noted our conclusion of the review that we conducted on the bounties issue and we have conveyed — through diplomatic, intelligence, and military channels — strong, direct messages on this issue, but we are not specifically tying the actions we are taking today to that — to that matter. We are tying it to the SolarWinds and election interference matters.

I did want to report to you, however, our finding on this, which is: There is an assessment that Russian intelligence officers did seek to encourage Taliban attacks against U.S. and coalition personnel, including through financial incentives and compensation, but because of the low- to moderate-confidence element of this, our focus is on sending a clear message to Russia about the steps the United States would take in response to such behavior were it to continue.

On the question of the PNGs: The United States is expelling these 10 Russian individuals because we have determined that they were acting in a manner inconsistent with their status in the United States.

And I will leave it at that and turn it over [senior administration official].

SENIOR ADMINISTRATION OFFICIAL: Yeah, thanks. On the question about the June 14 date, you are correct. The sovereign debt prohibitions come into effect on June 14 of this year. The rationale for this date is to allow time for financial institutions to understand and adapt to the measures we're taking and to facilitate an orderly process for these financial institutions to make any adjustments they choose.

So our intent here is to impose costs on the Russian government, but also to limit any spillovers to the U.S. or global financial markets.

Thanks.

Q Yeah, thanks. It's Eamon Javers with CNBC. Can you guys give us a little bit more detail on any calculations made about what the impact is of limiting access to ruble-denominated debt, in terms of the Russian ability — the Russian government's ability to fund itself? And how badly is it going to impact Russia's ongoing operations? I know you touched on it a little bit. I'm wondering if you have any more analysis or detail or numbers around that. Thanks.

SENIOR ADMINISTRATION OFFICIAL: I'm happy to take this if you'd like.

SENIOR ADMINISTRATION OFFICIAL: Yeah, please. Go for it.

SENIOR ADMINISTRATION OFFICIAL: Yeah, okay. So, Eamon, I would just — I would just refer you to history. This is — these aren't — these aren't theoretical calculations that we had to make. We just looked back to 2014 and 2015, also 2019, when similar measures were taken.

When you remove U.S. investors from the primary market, it causes a broader chilling effect. And what you've seen throughout history, even recent history — as speculation about this measure began to pick up — what you see is that Russia's borrowing costs rise, you see that there's capital flight, you see the currency weakens in tandem. And, you know, that has an impact on Russia's growth rate; it has an impact on Russia's inflation rate. Previously in 2014, Russia decided to spend some of its foreign reserves to defend the currency. Those are all choices that Russia will have to make.

But there is a negative feedback loop that is triggered when you remove U.S. investors from a sovereign debt market. And, as I mentioned before, the velocity of that feedback loop really is a function of what Russia decides to do next.

We hope — we hope for de-escalation. We hope for a stable and predictable way forward, but that's — that's really a matter for Russia.

In terms of — you asked about what markets are going to do. I don't — you know, we're not going to speculate about how markets are going to respond specifically. I would just repeat: We've demonstrated our resolve today to defend our national interests and defend core principles, but we've also done so, we think, in a strong and proportionate way.

Q Good morning. This is Dina Temple-Raston from NPR. I have two quick questions. The first is: If Russia escalates, what are you expecting to do?

And the second is: Do you expect that this is going to spur some changes in the way the federal government procures software? Is there going to be new rules, that sort of thing?

SENIOR ADMINISTRATION OFFICIAL: I'll defer to my colleague on the second question, which is a very good question.

On the first, we're not going to speculate about what Russia's responses would be. We've made clear to the Russian government that we believe these responses are proportionate and measured, that there is more we could do, and we are not looking to escalate.

They have indicated publicly and in other formats that they would intend to respond to this,

and we will have to see what they choose to do. The United States reserves the right, of course, to take further action as necessary. But our view is that the best course forward at this point would be for us to, for the United States and Russia both, to get off of the ladder of escalation and find a stable way forward.

So, we will track closely the Russian government responses to this, and then make determinations from that on the way forward.

SENIOR ADMINISTRATION OFFICIAL: And on the second question — thank you. So defending against malicious cyber activities requires two components: them and us. And your question exactly spoke to the "us" portion.

So the SolarWinds incident highlighted the need to rapidly modernize federal cybersecurity. We've kicked that effort off already, focused on the nine federal agencies who were compromised with five specific efforts: requiring a rapid rollout of encryption and multi-factor authentication; requiring a rapid rollout of security in the cloud; ensuring logging and endpoint detection is in place; and ensuring effective, mature security operations centers will be put in place as well.

Those efforts will also be the hallmark of an upcoming executive order which will build on those with regard to setting standards for the software the U.S. government procures. As you know, the software the U.S. government procures is the same software and hardware used broadly by companies and governments in the U.S. and around the world.

So putting the muscle of U.S. spending on information technology behind building more secure software and hardware is a key step to help companies and governments in the U.S. and around the world have the benefit of more secure software and hardware and, over the longer-term, counter sophisticated malicious cyber activity, as we saw in SolarWinds.

Q A little bit more on the SolarWinds issue here. You know, there's been some discussion about whether or not a response is warranted, given that, by — by most accounts, it is a cyber espionage campaign, albeit a rather broad and successful one at that.

Could you just explain a little bit more about why the SolarWinds attack is deserving of such a response, given that the U.S. and its allies also engages in cyber espionage and there has been a lot of discussion about whether or not this is any way different than — than those activities? Thank you.

SENIOR ADMINISTRATION OFFICIAL: [Senior administration official], I'm happy to take

that one if you'd like.

SENIOR ADMINISTRATION OFFICIAL: Please, [senior administration official], go for it.

SENIOR ADMINISTRATION OFFICIAL: Thanks, Dustin. So the SVR's compromise of the SolarWinds software supply chain gave it the ability to spy on or potentially disrupt more than 16,000 computer systems worldwide. But there's really three core reasons that we saw the need to make clear that this behavior was unacceptable.

First, that broad scope and scale of the compromise, it's a national security and public safety concern.

Second, as you noted, the speed with which an actor can move from espionage to degrading or disrupting a network is at the blink of an eye, and a defender cannot move at that speed. And given the history of Russia's malicious activity in cyberspace and their reckless behavior in cyberspace, that was a key concern.

And finally, the hack placed an undue burden on the mostly private-sector victims who must bear the unusually high costs of mitigating this incident.

So, based on the three factors, we saw a need to make clear that activities like SolarWinds were reckless and unacceptable.

SENIOR ADMINISTRATION OFFICIAL: Thank you everyone. This is [senior administration official] again. This concludes our call. A friendly reminder that we are on background, attributed to "senior administration officials." And with the conclusion of this call, the embargo is lifted.

10:05 A.M. EDT